LINEAR CODES WITH TWO OR THREE WEIGHTS FROM SOME FUNCTIONS WITH LOW WALSH SPECTRUM IN ODD CHARACTERISTIC

GUANGKUI XU AND XIWANG CAO

Abstract. Linear codes with few weights have applications in authentication codes, secrete sharing schemes, association schemes, consumer electronics and data storage system. In this paper, several classes of linear codes with two or three weights are obtained from some functions with low Walsh spectrum in odd characteristic. Numerical results show that some of the linear codes obtained are optimal or almost optimal in the sense that they meet certain bounds on linear codes.

1. Introduction

Let p be a prime and $q = p^m$ for some positive integer m. Let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. An $[n, \kappa, d]$ linear code $\mathcal{C}$ is a κ-dimension linear subspace of $\mathbb{F}_p^n$ with minimum nonzero Hamming weight d. Let A_i be the number of codewords with the Hamming weight i in the code $\mathcal{C}$ of length n. The *weight enumerator* of $\mathcal{C}$ is defined by

$$1 + A_1 z + A_2 z^2 + \cdots + A_n z^n.$$

The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the *weight distribution* of the code $\mathcal{C}$. It is well known that the error correcting capabilities of a linear code depend on the minimum weight of the code. If more is known about the weight distribution of a code we can provide information about the error probability of error detection and correction with respect to some error detection and error correction algorithms. In general, it is difficult to determine the weight distribution of a given linear code $\mathcal{C}$. A linear code $\mathcal{C}$ is called a t-weight code if the number of nonzero A_i in the sequence $(1, A_1, A_2, \cdots, A_n)$ is equal to t. An $[n, \kappa, d]$ linear code $\mathcal{C}$ is called optimal if its parameters n, κ and d meet a bound on linear codes [25, Chapter 2]. An $[n, \kappa, d]$ linear code $\mathcal{C}$ is called almost optimal if $[n, \kappa, d+1]$ meets a bound on linear codes [25, Chapter 2].

Linear codes with a few weights have applications have applications in secret sharing [1, 5, 35], authentication codes [14], association schemes [2], and strongly regular graphs [3]. Some interesting two-weight and three-weight codes can be found in [10, 13, 18, 19, 22, 29, 36] and [39].

Let k be a divisor of m. The trace map from $\mathbb{F}_{p^m}$ onto its subfield $\mathbb{F}_{p^k}$ is defined as

$$\mathrm{Tr}_k^n(x) = x + x^{p^k} + x^{p^{2k}} + \cdots + x^{p^{n-k}}.$$

Key words and phrases. Plateaued functions, linear codes, Walsh spectrum, weight distribution.

The absolute trace map (i.e., for k=1) is simply denoted by $\mathrm{Tr}(x)=\sum_{i=0}^{n-1} x^{p^i}$.

For a prime p, let f be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. The *Walsh transform* of f is defined by

$$\widehat{\chi}_f(a)=\sum_{x\in\mathbb{F}_{p^m}} \omega_p^{f(x)-\mathrm{Tr}(ax)}, a\in\mathbb{F}_{p^m},$$

where $\omega_p=e^{2\pi\sqrt{-1}/p}$ is a primitive p-th root of unity. The values $\widehat{\chi}_f(a), a\in\mathbb{F}_{p^n}$ are called the *Walsh coefficients* of f. The *Walsh spectrum* of f is the multiset $\{\widehat{\chi}_f(a), a\in\mathbb{F}_{p^m}\}$.

Walsh transform is a basic tool to investigate the properties of cryptography functions. The functions with low Walsh spectrum have received a lot of attention in the literature on cryptography, coding theory, communication, sequence design and graph theory. A function f from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ is *bent* if $|\widehat{\chi}_f(a)|=p^{m/2}$ for all $a\in\mathbb{F}_{p^m}$. A p-ary bent function $f(x)$ is called *regular* if $\widehat{\chi}_f(a)=p^{m/2}\omega_p^{f^*(a)}$ for any $a\in\mathbb{F}_{p^m}$, where the function $f^*(x)$ is called the dual of $f(x)$. A bent function $f(x)$ is called *weakly regular* if there is a complex μ with unit magnitude such that $\widehat{\chi}_f(a)=p^{m/2}\mu\omega_p^{f^*(a)}$. For an integer $0\leq l\leq m$, if $|\widehat{\chi}_f(a)|\in\{0,p^{\frac{m+l}{2}}\}$ for all $a\in\mathbb{F}_{p^m}$, then we call f *l-plateaued*. Plateaued functions were introduced by Zheng and Zhang as good candidates for designing cryptographic functions since they possess desirable various cryptographic characteristics [37]. It should be noted that binary l-plateaued functions exist only when m and l have the same parity. For $l\in\{0,1,2\}$, l-plateaued functions have been actively studied and have attractive much attention due to their cryptographic, algebraic, and combinatorial properties. The case $l=0$ corresponds to bent functions by definition. For 1-plateaued functions the term near-bent function is common (see [8]), binary 1-plateaued and 2-plateaued functions are referred to as semi-bent functions in [30]. For more details on bent and l-plateaued functions, see [4, 6, 7, 9, 24, 26, 27, 31] and [38].

For a subset $D=\{d_1,d_2,\cdots,d_n\}$ of $\mathbb{F}_q$, we can define a linear code $\mathcal{C}_{\mathcal{D}}$ of length n over $\mathbb{F}_p$ by

$$\mathcal{C}_D=\{\mathbf{c}_a=(\mathrm{Tr}(ad_1),\mathrm{Tr}(ad_2),\cdots,\mathrm{Tr}(ad_n))\mid a\in\mathbb{F}_q\}, \tag{1.1}$$

and call D the *defining set* of this code $\mathcal{C}_{\mathcal{D}}$.

This construction technique can generate many classes of known codes with a few weights by selecting the suitable defining set D [14, 15, 16, 23] and [33]. In [17], a different method of constructing linear codes using specific classes of 2-designs was studied, and linear codes with a few weights were constructed from almost difference sets, difference sets, and a type of 2-designs associated to semi-bent functions. In [20], a class of binary three-weight linear codes was constructed by using the Weil sum $\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}(ax^{2^h+1}+bx)}$. Recently, several classes of p-ary linear codes with two or three weights have been obtained from some p-ary bent functions in [21, 32] and [40].

Based on the above mentioned work, this paper makes further endeavors to construct two or three-weight linear codes by selecting the defining set $D\subseteq\mathbb{F}_q$. First, a class of ternary linear codes with two weights is constructed from the preimage of a class of ternary monomials with four-valued Walsh transform. Second, two class of ternary three-weight linear codes are obtained from a class of quadratic ternary near-bent and 2-plateaued functions. Moreover, the weight distributions of these ternary linear codes are completely determined. Numerical results show that

the proposed class contains some optimal or almost optimal linear codes. Third, by analyzing the values of some Weil sum, a class of p-ary three-weight linear codes is constructed.

The organization of this paper is as follows. In Section 2, a class of ternary two-weight linear codes and two classes of ternary three-weight linear codes are provided. In Section 3, a class of p-ary three-weight linear codes are obtained by using some Weil sum. Conclusions are finally drawn in Section 4 .

2. Ternary linear codes with two or three weights from some ternary functions with low Walsh spectrum

In [32] and [40], the authors provided several classes of p-ary linear codes with two or three weights from bent functions over the finite field $\mathbb{F}_p$, where p is an odd prime. In this section, we construct several classes of ternary linear codes with two or three weights from some ternary functions with low Walsh spectrum.

Let $f(x)$ be a ternary function from $\mathbb{F}_{3^m}$ to $\mathbb{F}_3$ with $f(-x) = f(x)$ and $f(0) = 0$. In this section, the defining set D_b of the ternary code $\mathcal{C}_{D_b}$ is given by

$$D_b = \{x \in \mathbb{F}_{3^m}^* : f(x) = b\}. \tag{2.1}$$

where $b \in \mathbb{F}_3$. Denote $n_b = |D_b|$. Clearly, the length n of the code $\mathcal{C}_{D_b}$ is equal to n_b. We compute

$$\begin{aligned}
n_b =& \frac{1}{3} \sum_{x\in\mathbb{F}_{3^m}^*} \sum_{y\in\mathbb{F}_3} \omega_3^{y(f(x)-b)} \\
=& \frac{1}{3} \sum_{x\in\mathbb{F}_{3^m}^*} (1 + \omega_3^{-b}\omega_3^{f(x)} + \omega_3^{b}\omega_3^{-f(x)}) \\
=& \begin{cases} 3^{m-1} - 1 + \frac{1}{3}(\widehat{\chi}_f(0) + \overline{\widehat{\chi}_f(0)}) & \text{if } b = 0, \\ 3^{m-1} + \frac{1}{3}(\omega_3^{-b}\widehat{\chi}_f(0) + \omega_3^{b}\overline{\widehat{\chi}_f(0)}) & \text{if } b \neq 0. \end{cases}
\end{aligned} \tag{2.2}$$

Note that the Hamming weight $\mathrm{wt}(\mathbf{c}_a)$ of $\mathbf{c}_a$ is $n_b - N_a$, where

$$N_a = |\{x \in \mathbb{F}_{3^m}^* : f(x) = b \text{ and } \mathrm{Tr}(ax) = 0\}|$$

for each $a \in \mathbb{F}_{3^m}^*$. We have

$$\begin{aligned}
N_a =& \frac{1}{9} \sum_{x\in\mathbb{F}_{3^m}^*} (\sum_{y\in\mathbb{F}_3} \omega_3^{y(f(x)-b)})(\sum_{z\in\mathbb{F}_3} \omega_3^{z\mathrm{Tr}(ax)}) \\
=& \frac{1}{9} \sum_{x\in\mathbb{F}_{3^m}^*} (1 + \omega_3^{-b}\omega_3^{f(x)} + \omega_3^{b}\omega_3^{-f(x)})(1 + \omega_3^{\mathrm{Tr}(ax)} + \omega_3^{-\mathrm{Tr}(ax)}) \\
=& \frac{1}{9}(3^m - 3 - 3(\omega_3^{-b} + \omega_3^{b})) + \frac{1}{9}(\omega_3^{-b}\widehat{\chi}_f(0) + \omega_3^{b}\overline{\widehat{\chi}_f(0)} + 2(\omega_3^{-b}\widehat{\chi}_f(a) + \omega_3^{b}\overline{\widehat{\chi}_f(a)})) \\
=& \begin{cases} 3^{m-2} - 1 + \frac{1}{9}(\widehat{\chi}_f(0) + \overline{\widehat{\chi}_f(0)} + 2(\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)})) & \text{if } b = 0, \\ 3^{m-2} + \frac{1}{9}(\omega_3^{-b}\widehat{\chi}_f(0) + \omega_3^{b}\overline{\widehat{\chi}_f(0)} + 2(\omega_3^{-b}\widehat{\chi}_f(a) + \omega_3^{b}\overline{\widehat{\chi}_f(a)})) & \text{if } b \neq 0. \end{cases}
\end{aligned} \tag{2.3}$$

where the third identity holds because $f(-x) = f(x)$.

In general, it is difficult to determine the Walsh coefficients of a ternary function. When the ternary function f is selected properly, the code $\mathcal{C}_{D_b}$ may have only a few weights and have good parameters. We shall demonstrate this in the remainder of this section.

2.1. **A class of ternary linear codes with two weights.** Let $m=2k$ and k is a positive integer with $\gcd(k,3)=1$. In [28], Li and Yue studied the Walsh transform of the monomial function

$$f(x)=\mathrm{Tr}(\lambda x^{\frac{3^m-1}{4}}) \tag{2.4}$$

for $\lambda\in\mathbb{F}_{3^m}^*$ and determined the value distribution of the Walsh transform of $f(x)$ in terms of the Gauss periods. In this subsection, we shall present a class ternary linear codes with two weights whose the defining set is the preimage $f^{-1}(b)$ for each $b\in\mathbb{F}_3$.

First we recall some results obtained in [28, Theorems 3.3 (1) and 3.4 (1)].

Lemma 2.1. *Let $m=2k$ and k is a positive integer with $\gcd(k,3)=1$. Let $\lambda\in\mathbb{F}_{3^m}^*$ such that $\mathrm{Tr}_2^m(\lambda)$ is a square in $\mathbb{F}_9^*$.*

- **(i):** *If k is an even integer, then $\widehat{\chi}_f(0)=\frac{3^m+3}{4}$ and the value distribution of the Walsh transform of $f(x)=\mathrm{Tr}(\lambda x^{\frac{3^m-1}{4}})$ is given as follows:*

$$\widehat{\chi}_f(a)=\begin{cases}\frac{3^m+3}{4} & \textit{occurs } 1 \textit{ times},\\ -3^k+\frac{3^k+3}{4} & \textit{occurs } \frac{3^m-1}{2} \textit{ times},\\ -3^k\omega_3+\frac{3^k+3}{4} & \textit{occurs } \frac{3^m-1}{4} \textit{ times},\\ -3^k\omega_3^2+\frac{3^k+3}{4} & \textit{occurs } \frac{3^m-1}{4} \textit{ times}.\end{cases}$$

- **(ii):** *If k is an odd integer, then $\widehat{\chi}_f(0)=\frac{3^m+3}{4}$ and the value distribution of the Walsh transform of $f(x)=\mathrm{Tr}(\lambda x^{\frac{3^m-1}{4}})$ is given as follows:*

$$\widehat{\chi}_f(a)=\begin{cases}\frac{3^m+3}{4} & \textit{occurs } 1 \textit{ times},\\ 3^k-\frac{3^k-3}{4} & \textit{occurs } \frac{3^m-1}{2} \textit{ times},\\ 3^k\omega_3-\frac{3^k-3}{4} & \textit{occurs } \frac{3^m-1}{4} \textit{ times},\\ 3^k\omega_3^2-\frac{3^k-3}{4} & \textit{occurs } \frac{3^m-1}{4} \textit{ times}.\end{cases}$$

The main results of this subsection are described in the following two theorems.

Theorem 2.2. *Let $m=2k$ and k is an even positive integer with $\gcd(k,3)=1$. Let $\lambda\in\mathbb{F}_{3^m}^*$ such that $\mathrm{Tr}_2^m(\lambda)$ is a square in $\mathbb{F}_9^*$. Let f be defined as in (2.4) and D_b be defined as in (2.1).*

- **(i):** *If $b=0$, then $\mathcal{C}_{D_b}$ is a $[\frac{3^m-1}{2},m]$ ternary two-weight code with the weight distribution in Table 1.*
- **(ii):** *If $b\neq 0$, then $\mathcal{C}_{D_b}$ is a $[\frac{3^m-1}{4},m]$ ternary two-weight code with the weight distribution in Table 2.*

TABLE 1. The weight distribution of the codes of Theorem 2.2(i) and Theorem 2.3(i)

Weight w	Multiplicity A_w
0	1
$3^{m-1}-3^{k-1}$	$\frac{3^m-1}{2}$
$3^{m-1}+3^{k-1}$	$\frac{3^m-1}{2}$

TABLE 2. The weight distribution of the codes of Theorem 2.2(ii)

Weight w	Multiplicity A_w
0	1
$\frac{3^{m-1}-3^{k-1}}{2}$	$\frac{3^{m+1}-3}{4}$
$\frac{3^{m-1}+3^{k}}{2}$	$\frac{3^{m}-1}{4}$

Proof. (i) Note that $\widehat{\chi}_f(0) = \frac{3^m+3}{4}$. It follows from (2.2) that

$$n_0 = 3^{m-1} - 1 + \frac{1}{3}(\widehat{\chi}_f(0) + \overline{\widehat{\chi}_f(0)}) = \frac{3^m - 1}{2}.$$

Thus the length n of the code $\mathcal{C}_{D_0}$ is equal to $\frac{3^m-1}{2}$.

According to Lemma 2.1 (i) and (2.3), we have

$$\begin{aligned} N_a =& 3^{m-2} - 1 + \frac{1}{9}(\widehat{\chi}_f(0) + \overline{\widehat{\chi}_f(0)} + 2(\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)})) \\ =& 3^{m-2} - 1 + \frac{1}{9}(\frac{3^m+3}{2} + 2(\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)})) \\ =& \begin{cases} \frac{3^{m-1}-2\cdot 3^{k-1}-1}{2} & \text{if } \widehat{\chi}_f(a) = -3^k + \frac{3^k+3}{4}, \\ \frac{3^{m-1}+2\cdot 3^{k-1}-1}{2} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3 + \frac{3^k+3}{4}, \\ \frac{3^{m-1}+2\cdot 3^{k-1}-1}{2} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3^2 + \frac{3^k+3}{4}. \end{cases} \end{aligned}$$

This implies that

$$\mathrm{wt}(\mathbf{c}_a) = n_0 - N_a = \begin{cases} \frac{3^{m-1}+3^{k-1}}{2} & \text{if } \widehat{\chi}_f(a) = -3^k + \frac{3^k+3}{4}, \\ \frac{3^{m-1}-3^{k-1}}{2} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3 + \frac{3^k+3}{4}, \\ \frac{3^{m-1}-3^{k-1}}{2} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3^2 + \frac{3^k+3}{4}. \end{cases}$$

It is easy to determine the weight distribution of Table 1 by using the value distribution of the Walsh transform of $f(x) = \mathrm{Tr}(\lambda x^{\frac{3^m-1}{4}})$. Since $\mathrm{wt}(\mathbf{c}_a) > 0$ for each $a \in \mathbb{F}_{3^m}^*$, the dimension of this code is m.

(ii) Since the case for $b = 2$ can be similarly proved as the case for $b = 1$, hereafter we only give the proof for $b = 1$. Note that $\widehat{\chi}_f(0) = \frac{3^m+3}{4}$. When $b = 1$, it follows from (2.1) that the length n of the code $\mathcal{C}_{D_1}$ is given by

$$n = n_1 = 3^{m-1} + \frac{1}{3}(\omega_3^2\widehat{\chi}_f(0) + \omega_3\overline{\widehat{\chi}_f(0)}) = \frac{3^m - 1}{4}. \tag{2.5}$$

By Lemma 2.1 (i) and (2.3), for any $a \in \mathbb{F}_{3^m}^*$, we have

$$\begin{aligned} N_a =& 3^{m-2} + \frac{1}{9}(\omega_3^2\widehat{\chi}_f(0) + \omega_3\overline{\widehat{\chi}_f(0)} + 2(\omega_3^2\widehat{\chi}_f(a) + \omega_3\overline{\widehat{\chi}_f(a)})) \\ =& 3^{m-2} + \frac{1}{9}(-\frac{3^m+3}{4} + 2(\omega_3^2\widehat{\chi}_f(a) + \omega_3\overline{\widehat{\chi}_f(a)})) \\ =& \begin{cases} \frac{3^{m-1}+2\cdot 3^{k-1}-1}{4} & \text{if } \widehat{\chi}_f(a) = -3^k + \frac{3^k+3}{4}, \\ \frac{3^{m-1}-2\cdot 3^{k}-1}{4} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3 + \frac{3^k+3}{4}, \\ \frac{3^{m-1}+2\cdot 3^{k-1}-1}{4} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3^2 + \frac{3^k+3}{4}. \end{cases} \end{aligned} \tag{2.6}$$

Hence, it follows from (2.5) and (2.6) that

$$\mathrm{wt}(\mathbf{c}_a) = n_1 - N_a = \begin{cases} \frac{3^{m-1}-3^{k-1}}{2} & \text{if } \widehat{\chi}_f(a) = -3^k + \frac{3^k+3}{4}, \\ \frac{3^{m-1}+3^k}{2} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3 + \frac{3^k+3}{4}, \\ \frac{3^{m-1}-3^{k-1}}{2} & \text{if } \widehat{\chi}_f(a) = -3^k\omega_3^2 + \frac{3^k+3}{4}. \end{cases}$$

Applying the value distribution of the Walsh transform of $f(x) = \mathrm{Tr}(\lambda x^{\frac{3^m-1}{4}})$ in Lemma 2.1 (i) gives the desired weight distribution. It is easily seen that the dimension of the code is m, as $\mathrm{wt}(\mathbf{c}_a) > 0$ for each $a \in \mathbb{F}_{3^m}^*$. This completes the proof. $\square$

The following theorem deals with the case for odd k. Its proof is similar to that of Theorem 2.2 and is omitted.

Theorem 2.3. *Let $m = 2k$ and k is an odd positive integer with $\gcd(k, 3) = 1$. Let $\lambda \in \mathbb{F}_{3^m}^*$ such that $\mathrm{Tr}_2^m(\lambda)$ is a square in $\mathbb{F}_9^*$. Let f be defined as in (2.4) and D_b be defined as in (2.1).*

- **(i):** *If $b = 0$, then $\mathcal{C}_{D_b}$ is a $[\frac{3^m-1}{2}, m]$ ternary two-weight code with the weight distribution in Table 1.*
- **(ii):** *If $b \neq 0$, then $\mathcal{C}_{D_b}$ is a $[\frac{3^m-1}{4}, m]$ ternary two-weight code with the weight distribution in Table 3.*

Table 3. The weight distribution of the codes of Theorem 2.3(ii)

Weight w	Multiplicity A_w
0	1
$\frac{3^{m-1}+3^{k-1}}{2}$	$\frac{3^{m+1}-3}{4}$
$\frac{3^{m-1}-3^k}{2}$	$\frac{3^m-1}{4}$

Example 2.4. Let $m = 4$, $k = 2$, and $f(x) = \mathrm{Tr}(x^{20})$.

- **(i):** The code $\mathcal{C}_{D_0}$ in Theorem 2.2 (i) has parameters $[40, 4, 24]$ and weight enumerator $1 + 40z^{24} + 40z^{30}$. The best linear code of length 40 and dimension 4 over $\mathbb{F}_3$ has minimum weight 27.
- **(ii):** The code $\mathcal{C}_{D_1}$ in Theorem 2.2 (ii) has parameters $[20, 4, 12]$ and weight enumerator $1 + 60z^{12} + 20z^{18}$. This code is optimal due to the Griesmer bound.

Example 2.5. Let $m = 10$, $k = 5$, and $f(x) = \mathrm{Tr}(x^{14762})$.

- **(i):** The code $\mathcal{C}_{D_0}$ in Theorem 2.3 (i) has parameters $[29524, 10, 19602]$ and weight enumerator $1 + 29524z^{19602} + 29524z^{19764}$.
- **(ii):** The code $\mathcal{C}_{D_1}$ in Theorem 2.3 (ii) has parameters $[14762, 10, 9720]$ and weight enumerator $1 + 14762z^{9720} + 44286z^{9882}$.

2.2. **Two class of ternary linear codes with three weights.** Below, we shall select some proper ternary plateaued functions to construct ternary linear codes $\mathcal{C}_{D_0}$ with three weights, where D_0 is defined as in (2.1). The following lemma was proved in [34, Theorem 2].

Lemma 2.6. *Let m be a positive integer with $m > 3$ and $\lambda, u, v \in \mathbb{F}_{3^m}^*$. The ternary function f is defined as*

$$f(x) = \mathrm{Tr}(\lambda x^2) + \mathrm{Tr}(ux)\mathrm{Tr}(vx). \tag{2.7}$$

(i): *If $\mathrm{Tr}(\frac{uv}{\lambda}) = 2$, $\mathrm{Tr}(\frac{u^2}{\lambda}) = 1$ and $\mathrm{Tr}(\frac{v^2}{\lambda}) = 1$, then $f(x)$ is near-bent. Moreover, for $a \in \mathbb{F}_{3^m}$,*

(2.8)
$$\widehat{\chi}_f(a) = \begin{cases} \eta(\lambda)(-1)^m i^{m+1} 3^{\frac{m+1}{2}} \omega_3^{-\mathrm{Tr}(\frac{a^2}{\lambda})} & \text{if } (\mathrm{Tr}(\frac{au}{\lambda})\mathrm{Tr}(\frac{av}{\lambda})) = (0,0), \\ \eta(\lambda)(-1)^m i^{m+1} 3^{\frac{m+1}{2}} \omega_3^{-\mathrm{Tr}(\frac{a^2}{\lambda})+1} & \text{if } (\mathrm{Tr}(\frac{au}{\lambda}), \mathrm{Tr}(\frac{av}{\lambda})) = (1,1) \text{ or } (2,2), \\ 0 & \text{otherwise,} \end{cases}$$

where $i = \sqrt{-1}$ and η is the quadratic character of $\mathbb{F}_{3^n}$.

(ii): *If If $\mathrm{Tr}(\frac{uv}{\lambda}) = 1$, $\mathrm{Tr}(\frac{u^2}{\lambda}) = 0$ and $\mathrm{Tr}(\frac{v^2}{\lambda}) = 0$, then $f(x)$ is a 2-plateaued function. Moreover, for $a \in \mathbb{F}_{3^m}$,*

$$\widehat{\chi}_f(a) = \begin{cases} \eta(\lambda)(-1)^{m-1} i^m 3^{\frac{m}{2}+1} \omega_3^{-\mathrm{Tr}(\frac{a^2}{\lambda})} & \text{if } (\mathrm{Tr}(\frac{au}{\lambda}), \mathrm{Tr}(\frac{av}{\lambda})) = (0,0), \\ 0 & \text{otherwise.} \end{cases} \tag{2.9}$$

Two classes of ternary linear codes $\mathcal{C}_{D_0}$ with three weights can be presented in the following two theorems.

Theorem 2.7. *Let m be a positive integer with $m > 3$ and $\lambda \in \mathbb{F}_{3^m}^*$. Let $u, v \in \mathbb{F}_{3^m}^*$ such that $\mathrm{Tr}(\lambda^{-1}uv) = 2$, $\mathrm{Tr}(\lambda^{-1}u^2) = 1$, $\mathrm{Tr}(\lambda^{-1}v^2) = 1$. Let f be defined as in (2.7) and D_0 be defined as in (2.1).*

(i): *If m is even, then $\mathcal{C}_{D_0}$ is a $[3^{m-1} - 1, m]$ three-weight ternary code with the weight distribution in Table 4.*

(ii): *If m is odd, then $\mathcal{C}_{D_0}$ is a $[3^{m-1} + 2\varepsilon\eta(\lambda)3^{\frac{m-1}{2}} - 1, m]$ three-weight ternary code with the weight distribution in Table 5, where $\varepsilon = 1$ if $m \equiv 1 \pmod 4$ and $\varepsilon = -1$ if $m \equiv 3 \pmod 4$.*

Table 4. The weight distribution of the codes of Theorem 2.7(i)

Weight w	Multiplicity A_w
0	1
$2 \cdot 3^{m-2} - 2\eta(\lambda)3^{\frac{m}{2}-1}$	$3^{m-2} + \eta(\lambda)3^{\frac{m}{2}-1}$
$2 \cdot 3^{m-2}$	$3^m - 1 - 2 \cdot 3^{m-2}$
$2 \cdot 3^{m-2} + 2\eta(\lambda)3^{\frac{m}{2}-1}$	$3^{m-2} - \eta(\lambda)3^{\frac{m}{2}-1}$

Table 5. The weight distribution of the codes of Theorem 2.7(ii)

Weight w	Multiplicity A_w
0	1
$2 \cdot 3^{m-2} + 4\varepsilon\eta(\lambda)3^{\frac{m-3}{2}}$	$2 \cdot 3^{m-1}$
$2 \cdot 3^{m-2}$	$3^{m-2} + 2\varepsilon\eta(\lambda)3^{\frac{m-3}{2}} - 1$
$2 \cdot 3^{m-2} + 6\varepsilon\eta(\lambda)3^{\frac{m-3}{2}}$	$2 \cdot 3^{m-2} - 2\varepsilon\eta(\lambda)3^{\frac{m-3}{2}}$

Proof. (i) Note that $\mathrm{Tr}(\lambda^{-1}uv) = 2$, $\mathrm{Tr}(\lambda^{-1}u^2) = 1$ and $\mathrm{Tr}(\lambda^{-1}v^2) = 1$. By Lemma 2.6 (i), we have $\widehat{\chi}_f(0) + \overline{\widehat{\chi}_f(0)} = 0$ as m is even. It follows from (2.2) that $n_0 = 3^{m-1} - 1$. Hence, the length n of the code $\mathcal{C}_{D_0}$ is equal to $n_0 = 3^{m-1} - 1$.

For $a \in \mathbb{F}_{3^m}^*$, to calculate N_a, we need to calculate $\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)}$ from (2.3).

If $m \equiv 0 \pmod 4$, then $i^{m+1} = i$. We evaluate $\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)}$ by distinguishing the following three cases.

When $(\mathrm{Tr}(\frac{au}{\lambda}), \mathrm{Tr}(\frac{av}{\lambda})) = (0,0)$, it follows from (2.8) that

$$\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)} = \begin{cases} 0 & \text{if } \mathrm{Tr}(\frac{a^2}{\lambda}) = 0, \\ \eta(\lambda)3^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\frac{a^2}{\lambda}) = 1, \\ -\eta(\lambda)3^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\frac{a^2}{\lambda}) = 2. \end{cases}$$

When $(\mathrm{Tr}(\frac{au}{\lambda}), \mathrm{Tr}(\frac{av}{\lambda})) = (1,1)$ or $(2,2)$, it follows from (2.8) that

$$\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)} = \begin{cases} -\eta(\lambda)3^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\frac{a^2}{\lambda}) = 0, \\ \eta(\lambda)3^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\frac{a^2}{\lambda}) = 1, \\ 0 & \text{if } \mathrm{Tr}(\frac{a^2}{\lambda}) = 2. \end{cases}$$

When $(\mathrm{Tr}(\frac{au}{\lambda}), \mathrm{Tr}(\frac{av}{\lambda})) \in \mathbb{F}_3^2 \setminus \{(0,0),(1,1),(2,2)\}$

$$\widehat{\chi}_f(a) + \overline{\widehat{\chi}_f(a)} = 0.$$

It then follows from (2.3) with $b = 0$ that

$$N_a \in \{3^{m-2} - 1, 3^{m-2} - 2\eta(\lambda)3^{\frac{m-2}{2}} - 1, 3^{m-2} + 2\eta(\lambda)3^{\frac{m-2}{2}} - 1\}.$$

Hence, the Hamming weight $\mathrm{wt}(\mathbf{c}_a)$ of $\mathbf{c}_a$ satisfies

$$\mathrm{wt}(\mathbf{c}_a) = n_0 - N_a \in \{2 \cdot 3^{m-2} - 2\eta(\lambda)3^{\frac{m-2}{2}}, 2 \cdot 3^{m-2}, 2 \cdot 3^{m-2} + 2\eta(\lambda)3^{\frac{m-2}{2}}\}.$$

This implies that the code $\mathcal{C}_{D_0}$ has three weights in the set above.

If $m \equiv 2 \pmod 4$, then $i^{m+1} = -i$. Similar as the proof above, we obtain

$$\mathrm{wt}(\mathbf{c}_a) = n_0 - N_a \in \{2 \cdot 3^{m-2} - 2\eta(\lambda)3^{\frac{m-2}{2}}, 2 \cdot 3^{m-2}, 2 \cdot 3^{m-2} + 2\eta(\lambda)3^{\frac{m-2}{2}}\}.$$

for any $a \in \mathbb{F}_{3^m}^*$. Note that $f(-x) = 0$ if $f(x) = 0$. This together $0 \notin D_0$ implies that the minimum distance of $\mathcal{C}_{D_0}^{\perp}$ is equal to 2. It is easy to see that the number $A_2^{\perp}$ of codewords with weight 2 in $\mathcal{C}_{D_0}^{\perp}$ is n. By solving the first three Pless Power Moments gives the desired weight distribution. Since $m > 3$, $\mathrm{wt}(\mathbf{c}_a) > 0$ for any $a \in \mathbb{F}_{3^m}^*$. Hence, the dimension of $\mathcal{C}_{D_0}$ is m.

(ii) The proof of (ii) is similar to that of (i) and is omitted. □

Example 2.8. Let $m = 4$. Let $\lambda = 1$, $u = -1$ and $v = 1$. Then the function defined by (2.7) is $f(x) = \mathrm{Tr}(x^2) - \mathrm{Tr}(x)^2$. Then the code $\mathcal{C}_{D_0}$ in Theorem 2.7 (i) has parameters $[26, 4, 12]$ and weight enumerator $1 + 12z^{12} + 62z^{18} + 6z^{24}$.

Example 2.9. Let $m = 5$. Let $\lambda = -1$, $u = -1$ and $v = 1$. Then the function defined by (2.7) is $f(x) = \mathrm{Tr}(-x^2) - \mathrm{Tr}(x)^2$ and the code $\mathcal{C}_{D_0}$ in Theorem 2.7 (ii) has parameters $[62, 5, 36]$ and weight enumerator $1 + 60z^{36} + 162z^{42} + 20z^{54}$, while the optimal ternary code has parameters $[62, 5, 39]$.

Theorem 2.10. *Let m be a positive integer with $m > 4$ and $\lambda \in \mathbb{F}_{3^m}^*$. Let $u, v \in \mathbb{F}_{3^m}^*$ such that $\mathrm{Tr}(\lambda^{-1}uv) = 1$, $\mathrm{Tr}(\lambda^{-1}u^2) = 0$, $\mathrm{Tr}(\lambda^{-1}v^2) = 0$. Let D_0 be defined as in (2.1) and f be defined as in (2.7).*

(i): *If m is even, then $\mathcal{C}_{D_0}$ is a $[3^{m-1}-2\varepsilon\eta(\lambda)3^{\frac{m}{2}}-1, m]$ three-weight ternary code with the weight distribution in Table 6, where $\varepsilon = 1$ if $m \equiv 0 \pmod 4$ and $\varepsilon = -1$ if $m \equiv 2 \pmod 4$.*

(ii): *If m is odd, then $\mathcal{C}_{D_0}$ is a $[3^{m-1}-1, m]$ three-weight ternary code with the weight distribution in Table 7.*

TABLE 6. The weight distribution of the codes of Theorem 2.10(i)

Weight w	Multiplicity A_w
0	1
$2\cdot 3^{m-2}-4\varepsilon\eta(\lambda)3^{\frac{m}{2}-1}$	3^m-3^{m-2}
$2\cdot 3^{m-2}$	$3^{m-3}-2\varepsilon\eta(\lambda)3^{\frac{m}{2}-2}-1$
$2\cdot 3^{m-2}-6\varepsilon\eta(\lambda)3^{\frac{m}{2}-1}$	$2\cdot 3^{m-3}+2\varepsilon\eta(\lambda)3^{\frac{m}{2}-2}$

TABLE 7. The weight distribution of the codes of Theorem 2.10(ii)

Weight w	Multiplicity A_w
0	1
$2\cdot 3^{m-2}-2\eta(\lambda)3^{\frac{m+1}{2}-1}$	$3^{m-3}+\eta(\lambda)3^{\frac{m-3}{2}}$
$2\cdot 3^{m-2}$	$3^m-2\cdot 3^{m-3}-1$
$2\cdot 3^{m-2}+2\eta(\lambda)3^{\frac{m+1}{2}-1}$	$3^{m-3}-\eta(\lambda)3^{\frac{m-3}{2}}$

Proof. We just omit the proof here since it is similar to that of Theorem 2.7. □

Remark 2.11. It should be noted that if λ is a nonsquare in $\mathbb{F}_{3^4}^*$, the first conclusion in Theorem 2.10 is also true when $m = 4$.

Example 2.12. Let $m = 4$ and let α be the generator of $\mathbb{F}_{3^4}^*$ with $\alpha^4 - \alpha^3 - 1 = 0$. Let $\lambda = \alpha$, $u = \alpha^{16}$ and $v = \alpha^8$. Then the function defined by (2.7) is $f(x) = \mathrm{Tr}(\alpha x^2) + \mathrm{Tr}(\alpha^{16}x)\mathrm{Tr}(\alpha^8 x)$ and the code $\mathcal{C}_{D_0}$ in Theorem 2.10 (i) has parameters $[44, 4, 18]$ and weight enumerator $1 + 4z^{18} + 72z^{30} + 4z^{36}$.

Example 2.13. Let $m = 7$ and let α be the generator of $\mathbb{F}_{3^7}^*$ with $\alpha^7 + 2\alpha^2 + 1 = 0$. Let $\lambda = \alpha$, $u = \alpha$ and $v = \alpha^{17}$. Then the function defined by (2.7) is $f(x) = \mathrm{Tr}(\alpha x^2) + \mathrm{Tr}(\alpha x)\mathrm{Tr}(\alpha^{17}x)$ and the code $\mathcal{C}_{D_0}$ in Theorem 2.10 (ii) has parameters $[728, 7, 432]$ and weight enumerator $1 + 90z^{432} + 2024z^{486} + 72z^{540}$.

Recall that $f(x) = f(-x)$. Then the set D_0 defined as in (2.1) can be expressed as

$$D_0 = -\bar{D} \cup \bar{D}, \tag{2.10}$$

where $d_i d_j^{-1} \neq \pm 1$ for every pair of distinct elements d_i and d_j in $\bar{D}$. Selecting $\bar{D}$ as the defining set gives ternary three-weights codes, whose parameters and the weight distributions are given in the following two corollaries.

Corollary 2.14. *Let m be a positive integer with $m > 3$ and $\lambda \in \mathbb{F}_{3^m}^*$. Let $u, v \in \mathbb{F}_{3^m}^*$ such that $\mathrm{Tr}(\lambda^{-1}uv) = 2$, $\mathrm{Tr}(\lambda^{-1}u^2) = 1$, $\mathrm{Tr}(\lambda^{-1}v^2) = 1$. Let $\bar{D}$ be defined as in (2.10) and f be defined as in (2.7).*

(i): *If m is even, then $\mathcal{C}_{\bar{D}}$ is a $[\frac{3^{m-1}-1}{2}, m]$ three-weight ternary code with the weight distribution in Table 8.*

(ii): *If m is odd, then $\mathcal{C}_{\bar{D}}$ is a $[\frac{3^{m-1}-1}{2}+\varepsilon\eta(\lambda)3^{\frac{m-1}{2}}, m]$ three-weight ternary code with the weight distribution in Table 9, where $\varepsilon = 1$ if $m \equiv 1 \pmod 4$ and $\varepsilon = -1$ if $m \equiv 3 \pmod 4$.*

TABLE 8. The weight distribution of the codes of Corollary 2.14(i)

Weight w	Multiplicity A_w
0	1
$3^{m-2}-\eta(\lambda)3^{\frac{m}{2}-1}$	$3^{m-2}+\eta(\lambda)3^{\frac{m}{2}-1}$
3^{m-2}	$3^m-1-2\cdot 3^{m-2}$
$3^{m-2}+\eta(\lambda)3^{\frac{m}{2}-1}$	$3^{m-2}-\eta(\lambda)3^{\frac{m}{2}-1}$

TABLE 9. The weight distribution of the codes of Corollary 2.14(ii)

Weight w	Multiplicity A_w
0	1
$3^{m-2}+2\varepsilon\eta(\lambda)3^{\frac{m-3}{2}}$	$2\cdot 3^{m-1}$
3^{m-2}	$3^{m-2}+2\varepsilon\eta(\lambda)3^{\frac{m-3}{2}}-1$
$3^{m-2}+3\varepsilon\eta(\lambda)3^{\frac{m-3}{2}}$	$2\cdot 3^{m-2}-2\varepsilon\eta(\lambda)3^{\frac{m-3}{2}}$

Example 2.15. Let $m=4$. Let $\lambda=1$, $u=-1$ and $v=1$. Then $f(x)=\mathrm{Tr}(x^2)-\mathrm{Tr}(x)^2$ and the code $\mathcal{C}_{\bar{D}}$ in Corollary 2.14 (i) has parameters $[13,4,6]$ and weight enumerator $1+12z^6+62z^9+6z^{12}$. This code is almost optimal as the optimal ternary code has parameters $[13,4,7]$.

Example 2.16. Let $m=5$. Let $\lambda=-1$, $u=-1$ and $v=1$. Then $f(x)=\mathrm{Tr}(-x^2)-\mathrm{Tr}(x)^2$ and the code $\mathcal{C}_{\bar{D}}$ in Corollary 2.14 (ii) has parameters $[31,5,18]$ and weight enumerator $1+60z^{18}+162z^{21}+20z^{27}$. This code is optimal due to the Griesmer bound.

Corollary 2.17. *Let m be a positive integer with $m>4$ and $\lambda\in\mathbb{F}_{3^m}^*$. Let $u,v\in\mathbb{F}_{3^m}^*$ such that $\mathrm{Tr}(\lambda^{-1}uv)=1$, $\mathrm{Tr}(\lambda^{-1}u^2)=0$, $\mathrm{Tr}(\lambda^{-1}v^2)=0$. Let $\bar{D}$ be defined as in (2.10) and f be defined as in (2.7).*

(i): *If m is even, then $\mathcal{C}_{\bar{D}}$ is a $[\frac{3^{m-1}-1}{2}-\varepsilon\eta(\lambda)3^{\frac{m}{2}}, m]$ three-weight ternary code with the weight distribution in Table 10, where $\varepsilon=1$ if $m\equiv 0 \pmod 4$ and $\varepsilon=-1$ if $m\equiv 2 \pmod 4$.*

(ii): *If m is odd, then $\mathcal{C}_{\bar{D}}$ is a $[\frac{3^{m-1}-1}{2}, m]$ three-weight ternary code with the weight distribution in Table 11.*

TABLE 10. The weight distribution of the codes of Corollary 2.17(i)

Weight w	Multiplicity A_w
0	1
$3^{m-2}-2\varepsilon\eta(\lambda)3^{\frac{m}{2}-1}$	3^m-3^{m-2}
3^{m-2}	$3^{m-3}-2\varepsilon\eta(\lambda)3^{\frac{m}{2}-2}-1$
$3^{m-2}-3\varepsilon\eta(\lambda)3^{\frac{m}{2}-1}$	$2\cdot 3^{m-3}+2\varepsilon\eta(\lambda)3^{\frac{m}{2}-2}$

TABLE 11. The weight distribution of the codes of Corollary 2.17(ii)

Weight w	Multiplicity A_w
0	1
$3^{m-2}-\eta(\lambda)3^{\frac{m+1}{2}-1}$	$3^{m-3}+\eta(\lambda)3^{\frac{m-3}{2}}$
3^{m-2}	$3^m-2\cdot 3^{m-3}-1$
$3^{m-2}+\eta(\lambda)3^{\frac{m+1}{2}-1}$	$3^{m-3}-\eta(\lambda)3^{\frac{m-3}{2}}$

Example 2.18. Let $m=4$ and let α be the generator of $\mathbb{F}_{3^4}^*$ with $\alpha^4-\alpha^3-1=0$. Let $\lambda=\alpha$, $u=\alpha^{16}$ and $v=\alpha^8$. Then $f(x)=\mathrm{Tr}(\alpha x^2)+\mathrm{Tr}(\alpha^{16}x)\mathrm{Tr}(\alpha^8 x)$ and the code $\mathcal{C}_{\bar{D}}$ in Corollary 2.17 (i) has parameters $[22,4,9]$ and weight enumerator $1+4z^9+72z^{15}+4z^{18}$, while the optimal ternary code has parameters $[22,4,11]$.

Example 2.19. Let $m=5$ and let α be the generator of $\mathbb{F}_{3^5}^*$ with $\alpha^5-\alpha+1=0$. Let $\lambda=\alpha$, $u=\alpha$ and $v=\alpha^4$. Then $f(x)=\mathrm{Tr}(\alpha x^2)+\mathrm{Tr}(\alpha x)\mathrm{Tr}(\alpha^4 x)$ and the code $\mathcal{C}_{\bar{D}}$ in Corollary 2.17 (ii) has parameters $[40,5,18]$ and weight enumerator $1+12z^{18}+224z^{27}+6z^{36}$.

3. A class of p-ary three-weight linear codes

Let m and h be positive integers. Denote $d=\gcd(h,m)$. For $\lambda,a\in\mathbb{F}_{p^m}$, a Gold function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ is defined by

$$f(x)=\mathrm{Tr}(\lambda x^{p^h+1}).$$

Based on the fact that a quadratic p-ary bent function has full rank, Zhou et al. [40, Section III.B] have obtained a class of linear codes with two or three weights by using Gold class of bent functions. In this subsection, following the work of [40], we shall employ Gold class of plateaued functions whose rank is less than m to construct p-ary linear codes with three weights. Before dong this, we first recall several lemmas about the following Weil sum.

Let m and h be positive integers. Denote $d=\gcd(h,m)$. For $\lambda,a\in\mathbb{F}_{p^m}$, we denote by $S_h(\lambda,a)$ the Weil sum given by

$$S_h(\lambda,a)=\sum_{x\in\mathbb{F}_{p^m}}\omega_p^{\mathrm{Tr}(\lambda x^{p^h+1}+ax)}, \tag{3.1}$$

where $\omega_p=\frac{2\pi\sqrt{-1}}{p}$ is the complex primitive p-th root of unity.

Lemma 3.1. [11, Theorem 4.1] *For $m=2k$, the equation $\lambda^{p^h}x^{p^{2h}}+\lambda x=0$ is solvable for $x\in\mathbb{F}_{p^m}^*$ if and only if $\frac{m}{d}$ is even and $\lambda^{\frac{p^m-1}{p^d+1}}=(-1)^{\frac{k}{d}}$.*

In [11, 12], Coulter obtained explicit evaluations of the exponential sum (3.1), which are described in the following lemmas.

For $a=0$, the evaluation of the exponential sum (3.1) is given as follows.

Lemma 3.2. [11] *Let $\frac{m}{d}$ be even with $m=2k$. Then $S_h(\lambda,0)=S_h(-\lambda,0)$ and*

$$S_h(\lambda,0)=\begin{cases} p^{k+d} & \text{if } \lambda^{\frac{p^m-1}{p^d+1}}=(-1)^{\frac{k}{d}} \text{ and } \frac{k}{d} \text{ is odd,}\\ -p^{k+d} & \text{if } \lambda^{\frac{p^m-1}{p^d+1}}=(-1)^{\frac{k}{d}} \text{ and } \frac{k}{d} \text{ is even.}\end{cases} \tag{3.2}$$

For $a\neq 0$, the evaluation of the exponential sum (3.1) is given as follows.

Lemma 3.3. [12] *Let $\frac{m}{d}$ be even with $m = 2k$. Assume that $g(x) = \lambda^{p^h} x^{p^{2h}} + \lambda x$ is not a permutation polynomial over $\mathbb{F}_{p^m}$. Then for $a \neq 0$ we have $S_h(\lambda, a) = 0$ unless the equation $g(x) = -a^{p^h}$ is solvable. If this equation is solvable, then*

$$S_h(\lambda, a) = -(-1)^{\frac{k}{d}} p^{k+d} \omega_p^{-\mathrm{Tr}(\lambda x_0^{p^h+1})}, \tag{3.3}$$

where x_0 is some solution of the equation $g(x) = -a^{p^h}$.

Let $\frac{m}{d}$ be even with $m = 2k$ and $\lambda \in \mathbb{F}_{p^m}^*$ such that $\lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}}$. It follows from Lemmas 3.2, 3.3 and the definition of plateaued function that $f(x) = \mathrm{Tr}(\lambda x^{p^h+1})$ is a p-ary $2d$-plateaued function if $\lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}}$. A class of p-ary three-weight code can be obtained from this function. To this end, we need to prove the following two lemmas.

Lemma 3.4. *Let $\frac{m}{d}$ be even with $m = 2k$ and $\lambda \in \mathbb{F}_{p^m}^*$ such that $\lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}}$. Then*

$$S_h(\lambda, 0) = S_h(2\lambda, 0) = \cdots = S_h((p-1)\lambda, 0) = \begin{cases} p^{k+d} & \text{if } \lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}} \text{ and } \frac{k}{d} \text{ is odd,} \\ -p^{k+d} & \text{if } \lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}} \text{ and } \frac{k}{d} \text{ is even.} \end{cases}$$

Proof. Since $\frac{m}{d}$ is even, $p - 1 | \frac{p^m-1}{p^d+1}$. Hence, $(c\lambda)^{\frac{p^m-1}{p^d+1}} = \lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}}$ for each $c \in \mathbb{F}_p^*$. The desired result follows from Lemma 3.2. □

Lemma 3.5. *Let $\frac{m}{d}$ be even with $m = 2k$ and $\lambda \in \mathbb{F}_{p^m}^*$ such that $\lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}}$. For $a \in \mathbb{F}_{p^m}^*$, we have*

$$\sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}(y\lambda x^{p^h+1} + zax)} \in \{0, -(-1)^{\frac{k}{d}}(p-1)^2 p^{k+d}, (-1)^{\frac{k}{d}}(p-1)p^{k+d}\}.$$

Proof. Since $\frac{m}{d}$ is even and $\lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}}$, the equation $\lambda^{p^h} x^{p^{2h}} + \lambda x = 0$ is solvable for $x \in \mathbb{F}_{p^m}^*$ by Lemma 3.1. For $a \in \mathbb{F}_{p^m}^*$, we claim that the equation $\lambda^{p^h} x^{p^{2h}} + \lambda x + a^{p^h} = 0$ is solvable if and only if the equation $(y\lambda)^{p^h} x^{p^{2h}} + (y\lambda)x + (za)^{p^h} = 0$ is solvable for each $(y, z) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$. Assume that x_0 is a solution of the equation $\lambda^{p^h} x^{p^{2h}} + \lambda x + a^{p^h} = 0$. Clearly, x_0 is also a solution of the equation $y^{-1}z\lambda^{p^h} x^{p^{2h}} + y^{-1}z\lambda x + y^{-1}za^{p^h} = 0$. Then $y^{-1}z\lambda^{p^h} x_0^{p^{2h}} + y^{-1}z\lambda x_0 + y^{-1}za^{p^h} = 0$, which can be written as $\lambda^{p^h}(y^{-1}zx_0)^{p^{2h}} + \lambda(y^{-1}zx_0) + y^{-1}za^{p^h} = 0$ as $y, z \in \mathbb{F}_p^*$. It then follows that $(y\lambda)^{p^h}(y^{-1}zx_0)^{p^{2h}} + (y\lambda)(y^{-1}zx_0) + (za)^{p^h} = 0$. That is to say, the equation $(y\lambda)^{p^h} x^{p^{2h}} + (y\lambda)x + (za)^{p^h} = 0$ has a solution $y^{-1}zx_0$. Conversely, if x_0 is a solution of the equation $(y\lambda)^{p^h} x^{p^{2h}} + (y\lambda)x + (za)^{p^h} = 0$, then $(y\lambda)^{p^h} x_0^{p^{2h}} + (y\lambda)x_0 + (za)^{p^h} = 0$. Note that $y, z \in \mathbb{F}_p^*$. Hence, we have $\lambda^{p^h}(z^{-1}yx_0)^{p^{2h}} + \lambda(z^{-1}yx_0) + a^{p^h} = 0$. This implies that $\lambda^{p^h} x^{p^{2h}} + \lambda x + a^{p^h} = 0$ has a solution $z^{-1}yx_0$.

If the equation $\lambda^{p^h} x^{p^{2h}} + \lambda x + a^{p^h} = 0$ has no solutions in $\mathbb{F}_{p^m}$, by Lemma 3.3 and the discussions above, then we have

$$\sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}(y\lambda x^{p^h+1} + zax)} = 0.$$

If the equation $\lambda^{p^h} x^{p^{2h}} + \lambda x + a^{p^h} = 0$ has a solution x_0 in $\mathbb{F}_{p^m}$, then we know that $(y\lambda)^{p^h} x^{p^{2h}} + (y\lambda)x + (za)^{p^h} = 0$ has a solution $y^{-1}zx_0$ from the discussions above. It follows from (3.3) that

$$\begin{aligned}
&\sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}(y\lambda x^{p^h+1}+zax)} \\
&= -(-1)^{\frac{k}{d}} p^{k+d} \sum_{z\in\mathbb{F}_p^*}\sum_{y\in\mathbb{F}_p^*} \omega_p^{-\mathrm{Tr}(y\lambda(y^{-1}zx_0)^{p^h+1})} \\
&= -(-1)^{\frac{k}{d}} p^{k+d} \sum_{z\in\mathbb{F}_p^*}\sum_{y\in\mathbb{F}_p^*} \omega_p^{-y^{-1}z^2\mathrm{Tr}(\lambda x_0^{p^h+1})} \\
&= \begin{cases} -(-1)^{\frac{k}{d}}(p-1)^2 p^{k+d} & \text{if } \mathrm{Tr}(\lambda x_0^{p^h+1}) = 0, \\ (-1)^{\frac{k}{d}}(p-1)p^{k+d} & \text{if } \mathrm{Tr}(\lambda x_0^{p^h+1}) \neq 0. \end{cases}
\end{aligned}$$

Hence,

$$\sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}(y\lambda x^{p^h+1}+zax)} \in \{0, -(-1)^{\frac{k}{d}}(p-1)^2p^{k+d}, (-1)^{\frac{k}{d}}(p-1)p^{k+d}\}.$$

for each $a \in \mathbb{F}_{p^m}^*$.

□

Let h be positive integer $1 \le h < k$, where $m = 2k > 4$ is an even integer. Define

$$D = \{x \in \mathbb{F}_{p^m}^* : \mathrm{Tr}(\lambda x^{p^h+1}) = 0\}, \tag{3.4}$$

where $\lambda \in \mathbb{F}_{p^m}^*$.

Our main result of this subsection is the following.

Theorem 3.6. *Let h be positive integer $1 \le h < k$, where $m = 2k > 4$ is an even integer. Let D be defined in (3.4), where $\lambda \in \mathbb{F}_{p^m}^*$. Define $d = \gcd(h, m)$. Assume that $\frac{m}{d}$ be even and $\lambda^{\frac{p^m-1}{p^d+1}} = (-1)^{\frac{k}{d}}$.*

- **(i):** *If $\frac{k}{d}$ is odd, then $\mathcal{C}_D$ is a $[p^{m-1} + (p-1)p^{k+d-1} - 1, m, (p-1)p^{m-2}]$ three-weight code with the weight distribution in Table 12.*
- **(ii):** *If $\frac{k}{d}$ is even, then $\mathcal{C}_D$ is a $[p^{m-1} - (p-1)p^{k+d-1} - 1, m, (p-1)p^{m-2} - p(p-1)p^{k+d-2}]$ three-weight code with the weight distribution in Table 13.*

TABLE 12. The weight distribution of the codes of Theorem 3.6(i)

Weight w	Multiplicity A_w
0	1
$(p-1)p^{m-2}$	$\frac{(p^{m-2}+p^{k+d-1})(p^{m-2}-p^{k+d-2})}{p^{m+2d-3}}$
$(p-1)p^{m-2} + (p-1)^2p^{k+d-2}$	$p^m - 1 - \frac{(p^{m-1}+p^{k+d-1})(p^{m-2}-p^{k+d-2})}{p^{m+2d-3}}$
$(p-1)p^{m-2} + p(p-1)p^{k+d-2}$	$\frac{(p-1)p^{m-2}(p^{m-2}-p^{k+d-2})}{p^{m+2d-3}}$

TABLE 13. The weight distribution of the codes of Theorem 3.6(ii)

Weight w	Multiplicity A_w
0	1
$(p-1)p^{m-2}-p(p-1)p^{k+d-2}$	$\frac{(p-1)p^{m-2}(p^{m-2}+p^{k+d-2})}{p^{m+2d-3}}$
$(p-1)p^{m-2}-(p-1)^2p^{k+d-2}$	$p^m-1-\frac{(p^{m-1}-p^{k+d-1})(p^{m-2}+p^{k+d-2})}{p^{m+2d-3}}$
$(p-1)p^{m-2}$	$\frac{(p^{m-2}-p^{k+d-1})(p^{m-2}+p^{k+d-2})}{p^{m+2d-3}}$

Proof. We only give the proof of (i) since the other can be proven in a similar manner. Denote $n_D = |D \cup \{0\}|$. We have

$$\begin{aligned} n_D =&\frac{1}{p}\sum_{x\in\mathbb{F}_{p^m}}\sum_{y\in\mathbb{F}_p}\omega_p^{y\mathrm{Tr}(\lambda x^{p^h+1})}\\ =&\frac{1}{p}\sum_{x\in\mathbb{F}_{p^m}}(1+\omega_p^{\mathrm{Tr}(\lambda x^{p^h+1})}+\omega_p^{2\mathrm{Tr}(\lambda x^{p^h+1})}+\cdots+\omega_p^{(p-1)\mathrm{Tr}(\lambda x^{p^h+1})})\\ =&p^{m-1}+\frac{1}{p}(S_h(\lambda,0)+S_h(2\lambda,0)+\cdots+S_h((p-1)\lambda,0)). \end{aligned}$$

Note that $\frac{k}{d}$ is odd and $\lambda^{\frac{p^m-1}{p^d+1}}=(-1)^{\frac{k}{d}}$. It then follows from Lemma 3.4 that

$$n = n_D - 1 = p^{m-1}+(p-1)p^{k+d-1}-1.$$

Note that the Hamming weight $\mathrm{wt}(\mathbf{c}_a)$ is $n_D - N_a$, where

$$N_a = |\{x\in\mathbb{F}_{p^m} : \mathrm{Tr}(\lambda x^{p^h+1})=0 \text{ and } \mathrm{Tr}(ax)=0\}|$$

for each $a\in\mathbb{F}_{p^m}^*$. We have

$$\begin{aligned} N_a =&\frac{1}{p^2}\sum_{x\in\mathbb{F}_{p^m}}(\sum_{y\in\mathbb{F}_p}\omega_p^{y\mathrm{Tr}(\lambda x^{p^h+1})})(\sum_{z\in\mathbb{F}_p}\omega_p^{z\mathrm{Tr}(ax)})\\ =&p^{m-2}+\frac{1}{p^2}(\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^m}}\omega_p^{y\mathrm{Tr}(\lambda x^{p^h+1})})+\frac{1}{p^2}\sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^m}}\omega_p^{\mathrm{Tr}(y\lambda x^{p^h+1}+zax)}.\\ =&p^{m-2}+\frac{1}{p^2}(\sum_{y\in\mathbb{F}_p^*}S_h(y\lambda,0))+\frac{1}{p^2}\sum_{y\in\mathbb{F}_p^*}\sum_{z\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_{p^m}}\omega_p^{\mathrm{Tr}(y\lambda x^{p^h+1}+zax)}. \quad (3.5) \end{aligned}$$

It follows from Lemmas 3.4 and 3.5 that

$$N_a\in\{p^{m-2}+(p-1)p^{k+d-2}, p^{m-2}+(p-1)^2p^{k+d-2}, p^{m-2}\}.$$

Hence, for any $a\in\mathbb{F}_{p^m}^*$, the weight of codeword $\mathbf{c}_a$ is given by

$$\mathrm{wt}(\mathbf{c}_a)=\{(p-1)p^{m-2}, (p-1)p^{m-2}+(p-1)^2p^{k+d-2}, (p-1)p^{m-2}+p(p-1)p^{k+d-2}\}$$

and the code $\mathcal{C}_D$ has three nonzero weights above. Since $m>4$, $\mathrm{wt}(\mathbf{c}_a)>0$ for each $a\in\mathbb{F}_{3^m}^*$. Therefore, the dimension of the code is m.

Since $0\notin D$, the minimum distance of $\mathcal{C}_D^\perp$ cannot be one. Note that $\mathrm{Tr}(\lambda(cx)^{p^h+1})=0$ for all $c\in\mathbb{F}_p^*$ if $\mathrm{Tr}(\lambda x^{p^h+1})=0$. Hence, the minimum distance of $\mathcal{C}_D^\perp$ is equal to 2. Moreover, we can know that the the number $A_2^\perp$ of codewords with weight 2 in

$\mathcal{C}_D^{\perp}$ is $\binom{p-1}{2}n$. In fact, for each $p-1$ distinct elements $u, 2u, \cdots, (p-1)u \in D$, we can obtain $\binom{p-1}{2}(p-1)$ codewords with weight 2 in $\mathcal{C}_D^{\perp}$. Define

$$w_1 = (p-1)p^{m-2}, w_2 = (p-1)p^{m-2}+(p-1)^2p^{k+d-2}, w_3 = (p-1)p^{m-2}+p(p-1)p^{k+d-2}.$$

We now determine the number A_{w_i} of codewords with weight w_i in $\mathcal{C}_D$. By calculating the first three Pless Power Moments [25, p.259], we have

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} = p^m - 1, \\ w_1A_{w_1} + w_2A_{w_2} + w_3A_{w_3} = (p-1)np^{m-1}, \\ w_1^2A_{w_1} + w_2^2A_{w_2} + w_3^2A_{w_3} = [(p-1)n((p-1)n+1) + 2\binom{p-1}{2}n]p^{m-2}. \end{cases}$$

Solving the above linear equations yields the desired weight distribution. □

Example 3.7. Let $m = 8$ and $h = 2$. Let $f(x) = \mathrm{Tr}(x^{10})$. Then the code $\mathcal{C}_D$ has parameters $[1700, 8, 972]$ and weight enumerator $1 + 60z^{972} + 6480z^{1134} + 20z^{1458}$.

Example 3.8. Let $m = 6$ and $h = 1$. Let α be the generator of $\mathbb{F}_{5^6}^*$ with $\alpha^6 + \alpha^4 - \alpha^3 + \alpha^2 + 2 = 0$. Let $\lambda = \alpha^3$. Clearly, $\lambda^{\frac{5^6-1}{6}} = \alpha^{7812} = -1$. Let $f(x) = \mathrm{Tr}(\alpha^3x^6)$. Then the code $\mathcal{C}_D$ has parameters $[3624, 6, 2500]$ and weight enumerator $1 + 144z^{2500} + 15000z^{2900} + 480z^{3000}$.

4. Conclusion

In this paper, several classes of linear codes with two or three weights are constructed from some functions with low Walsh spectrum in odd characteristic, which contain some optimal or almost optimal linear codes with parameters meeting certain bound on linear codes. The weight distributions of the these codes of this paper are determined by analyzing Walsh spectrum of some functions. Compared with other linear codes with two or three weights , the parameters of the linear codes with two or three weights of this paper are different from those obtained from bent functions in [17, 21, 32] and [40]. As applications, the two-weight codes in this paper can be used in strongly regular graphs with the method in [3], and some of the three-weight codes in this paper can be employed to construct secret sharing schemes with interesting access structures and association schemes introduced in [2].

Acknowledgement

This work was supported by the National Natural Science Foundation of China (Grants 11371011, 61403157 and 61572027).

References

[1] R. Anderson, C. Ding, T. Helleseth, and T. Kløve, "How to build robust shared control systems," *Designs, Codes Cryptography*, vol. 15, no. 2, pp. 111–124, Nov. 1998.

[2] A. R. Calderbank and J. M. Goethals, "Three-weight codes and association schemes," *Philips J. Res.*, vol. 39, pp. 143–152, 1984.

[3] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.*, vol. 18, pp. 97-122, 1986.

[4] C. Carlet and E. Prouff, "On plateaued functions and their constructions," in: Proceedings of Fast Software Encryption (FSE), Lecture Notes in Computer Science, vol. 2887, pp. 54–73, 2003.

[5] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inform. Theory*, vol. 51, no.6, pp. 2089–2102, 2005.

[6] C. Carlet, “Boolean functions for cryptography and error correcting codes,” *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, vol. 2, pp. 257–397, 2010.
[7] A. Çeşmelioğlu, W. Meidl, A. Pott, “Generalized Maiorana-McFarland class and normality of p-ary bent functions”, *Finite Fields Appl.*, vol. 24, no. 9, pp. 105–117, 2013.
[8] A. Çeşmelioğlu, G. McGuire, W. Meidl, “A construction of weakly and non-weakly regular bent functions,” *J. Combin. Theory Ser A* , vol. 119, pp. 420–429, 2012.
[9] S. Chee, S. Lee, and K. Kim, “Semi-bent functions,” in *Advances in CryptologyASI-ACRYPT'94*, pp. 105–118, Springer, 1995.
[10] S.-T. Choi, J.-Y. Kim, J.-S. No, and H. Chung, ”Weight distribution of some cyclic codes,” in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 2901-2903.
[11] R. S. Coulter, “Explicit evaluations of some Weil sums,” *Acta Arithmetica*, vol. 83, no. 03, pp. 241–251, 1998.
[12] R. S. Coulter, “Further evaluations of Weil sums”, *Acta Arithmetica*, vol. 3, pp. 217-226, 1998.
[13] B. Courteau and J. Wolfmann, “On triple-sum-sets and two or three weights codes,” *Discrete Math.*, vol. 50, pp. 179-191, 1984.
[14] C. Ding and X. Wang, “A coding theory construction of new systematic authentication codes”, *Theoretical Comput. Sci.*, vol. 330, no. 1, pp. 81–99, Jan. 2005.
[15] C. Ding and H. Niederreiter, “Cyclotomic linear codes of order 3,“ *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2274-2277, 2007.
[16] C. Ding, J. Luo and H. Niederreiter, “Two weight codes punctured from irreducible cyclic codes,” in: Proc. of the First International Workshop on Coding Theory and Cryptography, pp. 119-124. Singapore, World Scientific, 2008.
[17] C. Ding, “Linear codes from some 2-designs,” *IEEE Trans. Inform. Theory*, vol. 61, no. 6, pp. 3265-3275, June 2015.
[18] C. Ding, C. Li, N. Li, and Z. Zhou, “Three-Weight Cyclic Codes and Their Weight Distributions”, submitted for publication.
[19] C. Ding, J. Luo, and H. Niederreiter, ”Two weight codes punctured from irreducible cyclic codes,” in *Proc. 1st Int. Workshop Coding Theory Cryptography*, Y. Li, S. Ling, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, Eds., Singapore, 2008, pp. 119-124.
[20] K. Ding, C. Ding, “Binary linear codes with three weights,” *IEEE Trans. Inform. Theory*, vol. 18, no. 11, pp. 1879-1882, Novermber 2014.
[21] K. Ding and C. Ding, “A class of two-weight and three-weight codes and their applications in secret sharing,” *IEEE Trans. Inform. Theory*, DOI: 10.1109/TIT.2015.2473861.
[22] K. Feng and J. Luo, “Value distribution of exponential sums from perfect nonlinear functions and their applications,” *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3035-3041, Sep. 2007.
[23] Z. Heng and Q. Yue, “A class of binary linear codes with at most three weights”, *IEEE Commun. Lett*, vol. 19, no. 9, pp. 1488-1491, September 2015.
[24] Helleseth, T., Kholosha, A.“ Monomial and quadratic bent functions over the finite fields of odd characteristic,” *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2018–2032, 2006.
[25] W. C. Huffman and V. Pless, “Fundamentals of Error-Correcting Codes.” Cambridge, U.K.: Cambridge Univ. Press, 2003.
[26] K. Khoo, G. Gong, and D. R. Stinson, “A new characterization of semi-bent and bent functions on finite fields,” *Des. Codes Cryptogr.*, vol. 38, no. 2, pp. 279–295, 2006.
[27] W. Jia, X. Zeng, T.Helleset, ans C. Li, ”“A class of binomial bent functions over the finite fields of odd characteristic,” *IEEE Trans. Inform. Theory*, vol. 58, no. 9, pp. 6054–6063, 2012.
[28] C. Li and Q. Yue, “The Walsh transform of a class of monomial functions and cyclic codes,” *Cryptogr. Commun.*, vol. 7, no. 2, pp. 1936-2447, 2015.
[29] C. Li, Q. Yue, and F. Li, “Hamming weights of the duals of cyclic codes with two zeros,” *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 3895-3902, Jul. 2014.
[30] S. Mesnager, “On Semi-bent Functions and Related Plateaued Functions Over the Galois Field $\mathbb{F}_{2^n}$”, In: Open Problems in Mathematics and Computational Science, Springer, pp. 243–273, 2013.
[31] S. Mesnager, “Bent functions: fundamentals and results,” Springer, 2015, to appear.
[32] C. Tang and F. Qi, “Two-weight and three-weight linear codes from weakly regular bent functions”, arXiv:1507.06148.
[33] C. Xiang, “A Family of Three-Weight Binary Linear Codes”, arXiv:1505.07726.

[34] G. Xu and X. Cao, "Several classes of bent, near-bent and 2-plateaued functions over finite fields of odd characteristic", arXiv:1508.03415.

[35] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 206–212, Jan. 2006.

[36] X. Zeng, L. Hu, W. Jiang, Q. Yue, and X. Cao, "The weight distribution of a class of p-ary cyclic codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 56-73, Jan. 2010.

[37] Y. Zheng, X.M. Zhang, "Plateaued functions," in Advances in Cryptology ICICS 1999. Lecture Notes in Computer Science, vol. 1726 (Springer, Berlin, 1999), 284–300.

[38] Y. Zheng and X.M. Zhang, "Relationships between bent functions and complementary plateaued functions", Lecture Notes in Computer Science, **24** pp. 60–75, 1999.

[39] Z. Zhou and C. Ding, "A class of three-weight codes," *Finite Fields Appl.*, vol. 25, pp. 79-93, Jan. 2014.

[40] Z. Zhou, N. Li, C. Fan, T. Helleseth. "Linear Codes with Two or Three Weights From Quadratic Bent Functions," arXiv:1506.06830.

Guangkui Xu is the Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China, and also with the Department of Applied Mathematics, Huainan Normal University, Huainan 232038, China email: xuguangkuiy@163.com

Xiwang Cao is with School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China, and also with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China email: xwcao@nuaa.edu.cn